REMARKS

The foregoing amendments and the following remarks are responsive to the Office Action mailed July 28, 2004. Applicants respectfully request reconsideration of the present application. Claims 1, 3, 9, 22, 23 and 26 have been amended.

The Office Action rejected claims 1-4, 6-12, and 22-26 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,310,966 B1 by Dulude et al. (hereinafter "Dulude"). The Office Action rejected claim 5 under 35 U.S.C. §103(a) as being unpatentable over Dulude as applied to claim 1 above, and further in view of U.S. Patent No. 5,867,578 by Brickell et al. (hereinafter "Brickell").

Dulude discusses a method for authenticating an electronic transaction using biometric authentication. (Dulude, Abstract). The method includes pre-storing biometric data in a biometric database of a biometric certificate management system by receiving data corresponding to physical characteristics of registered users through a biometric input device, and authenticating subsequent electronic transactions by comparison of hash values in the digital signature with re-created hash values. (Dulude, Abstract). The digital signature is generated using data from 1) biometric data from the user, 2) identification data from the user, and 3) data from the electronic transaction. (Dulude, Abstract). The user is thus authenticated by comparison against the pre-stored biometric certificates of the physical characteristics of users in the biometric database. (Dulude, Abstract).

Claim 1, as amended, recites:

> A method of providing remote cryptographic services, the method comprising:
> a client requesting a cryptographic service;
> establishing a secure connection between the client and a biometric certification server (BCS);

receiving biometric data from a user; ~~and~~

the BCS ~~performing the cryptographic service~~ generating a disposable public key/private key pair if the user is authenticated based on the biometric authentication; and

the BCS performing the requested cryptographic service.

(Claim 1, as amended). Dulude does not teach generating a disposable public key/private key pair. Specifically, Dulude discloses a method as follows:

- A transaction transmission section 40 processes a user's biometric data 46 and transaction first data 50 (such as identification data 62), by a first hash function 52, to generate a first hashed value. (Dulude, Column 6, lines 1-5).
- The first hashed value is encrypted using the private key 56 of the first user to generate a digital signature 58. (Dulude, Column 6, lines 13-17).
- The digital signature is sent to the network 60. (Dulude, Column 6, line 17).
- The transaction transmission section 40 sends both the biometric data 46 and transaction first data 50 over the network 60, either unchanged or encrypted, to the transaction reception section 42. (Dulude, Column 5, lines 63-67).
- The identification data 62 is used to access a corresponding biometric certificate 68 stored in memory 66, which can be a biometric database or smart card. (Dulude, Column 6, lines 28-41).
- If no certificate exists in the memory, the user is not authenticated. (Dulude, Column 6, lines 45-57).

- If a certificate exists in memory, it is decrypted using the public key 70 of the certifying authority to obtain the decrypted registration biometric data 72 and the decrypted user public key 74. (Dulude, Column 6, lines 58-65).
- The decrypted user public key 74 is used to decrypt the digital signature 58. (Dulude, Column 6, lines 66-67).
- The first hash value is extracted and compared to a second hash value generated by the receiving section 42, to determine if both the transaction biometric and transaction first data are authentic and not modified during transaction. (Dulude, Column 7, lines 1-25).
- Further steps are taken by the receiving section to ensure that the electronic transaction is indeed from the indicated user. (Dulude, Column 7, lines 26-67; and Column 8, lines 1-27).

Thus, Dulude does not teach generating a disposable public key/private key pair upon authentication. Therefore, Applicants respectfully submit that claim 1, as amended, and dependent claims 2-9 are not anticipated by Dulude and are hence patentable.

The Office Action rejected 10-12 under 35 U.S.C. §102(e) as being anticipated by Dulude. Claim 10 recites:

A method of providing a certificate from a client to a server, the method comprising:
receiving a request for a certificate from the server;
forwarding the request to a biometric certification server (BCS);
receiving a biometric identification from the client and forwarding the biometric identification to the BCS;
if the biometric identification matches a registered user on the BCS, receiving a certificate including a public key of the client certified by the BCS; and

forwarding the certificate to the server, thereby identifying the client to the server.

The Office Action states that Dulude teaches forwarding the certificate to the server, thereby identifying the client to the server, at Dulude, Column 6, lines 50-65. Applicants respectfully submit that Dulude does not teach forwarding the certificate to the server. Dulude teaches storing the certificate in a biometric database or smart card memory 66 located in the receiving section 42. (Dulude, Figure 5). After extracting the certificate from database or memory 66, Dulude teaches sending the certificate to the biometric certificate extractor 64 associated with the receiving section 42, as shown in Figure 5, for decryption. (Dulude, Column 6, lines 59-63). Indeed, Dulude does not teach that the biometric certificate extractor 64 is located on an other server. Thus, the certificate is stored on the receiving section 42 and retrieved by the biometric certificate extractor 64, which is also located on the receiving section 42, and is thus not forwarded anywhere outside the receiving section 42. Applicants respectfully submit that Dulude does not teach forwarding the certificate to the server, thereby identifying the client to the server. Therefore, Applicants respectfully submit that claim 10, and dependent claims 11 and 12 are not anticipated by Dulude.

The Office Action rejected claims 13-21 under 35 U.S.C. §103(a) as being unpatentable over Dulude in view of U.S. Patent No. 6,587,946 B1 by Jakobsson (hereinafter "Jakobsson").

Jakobsson deals with the problem that arises when the primary recipient of an encrypted message is unavailable and the encrypted message needs to be made available to a secondary recipient who does not have the primary recipient's secret key. (Jakobsson, Column 3, lines 9 –15; Column 4, lines 59-67; Column 5, lines1-47).

Jakobsson discloses a method of forwarding an encrypted message sent to a primary recipient having a secret key to at least one secondary recipient. (Jakobsson, Abstract). The invention in Jakobsson is embodied in an email system 400 shown in Figure 4. (Jakobsson, Column 6, lines 49-65). Incoming email 110, which is public key encrypted, is sent to a primary recipient's mailbox 430. (Jakobsson, Column 6, lines 65-67). A group of proxy servers 420 is located on the email system 400 and maintains the email system 400. (Jakobsson, Column 7, lines 1-2; Figure 4). From this group of proxy servers 420, a quorum of proxy servers 425 is selected to act as the proxy. (Jakobsson, Column 7, lines 1-3). Portions of the primary recipient's secret key are dynamically shared among the proxy servers 425. (Jakobsson, Column 3, lines 37-41; Column 7, lines 25-28). Each of the proxy servers 425 transforms the message by applying the key portion to the encrypted message 110. (Jakobsson, Abstract). The result of the modification comprises a message secret to the proxy servers 425 but decryptable by at least one secondary recipient. (Jakobsson, Abstract). The resultant message is forwarded to at least one secondary recipient. (Jakobsson, Abstract).

The Office Action states that Jakobsson teaches a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection at column 4, lines 48-64. As discussed above, Jakobsson discloses that an encrypted email 110 arrives at a primary recipient's mailbox 430, and is transformed by proxy servers 425, such that it is decryptable at a secondary recipient's mailbox.. Jakobsson does not teach a crypto-proxy interface where requests for cryptographic function are received. Furthermore, claim 13 states that a request for cryptographic function is received from a client, to which data is returned after the cryptographic functions have

been performed. This means that in Jacobson's invention, the client must be the secondary recipient, to which the transformed message 110 is sent. Jakobsson does not disclose that there is a request for cryptographic function from the secondary recipient. Indeed, it is not clear whether the cryptographic function is initiated by the primary recipient, the proxy servers, or the secondary recipient.

Also, Applicants respectfully submit that the requisite motivation to combine Dulude and Jakobsson is lacking. The Office Action states that "[i]t would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Dulude et al by the teaching of Jakobsson because it is efficient, allows tight control over actions (by the use of quorum cryptography), does not require any pre-computation phase to set up shared keys, and has a trust model appropriate for a variety of settings...." (Office Action, page 7, lines 16-21). The Office Action refers to Jakobsson, column 3, lines 50-58 for this motivation.

Applicants respectfully submit while the invention disclosed in Jakobsson discusses the afore-mentioned advantages, the motivation is irrelevant to combine Jakobsson and Dulude. As discussed earlier, Jakobsson deals with a problem very different in nature to both Dulude and the present invention. It would not be obvious for person having ordinary skill in the art to look to Jakobsson, which discloses a "method and system for quorum controlled asymmetric proxy encryption" for modifying Dulude that deals with biometric certificates. (Jakobsson, Title). Therefore, Applicants respectfully submit that claim 13, and dependent claims 14-21 are not rendered obvious by Dulude, in view of Jakobsson.

The Office Action rejected claims 22 and 23 under 35 U.S.C. §102(e) as being anticipated by Dulude. Amended claim 22 recites:

An apparatus for permitting remote cryptographic functions comprising:
a crypto-API (application program interface) for receiving cryptographic function requests; ~~and~~
a cryptographic service provider for establishing a secure connection to a remote crypto-server, and having the crypto-server perform the cryptographic function; and
a sensor for receiving biometric data from a user, the biometric data sent to the crypto-server to authenticate the user, the remote crypto-server to generate a disposable public key/private key pair and perform the requested cryptographic function when the user is successfully authenticated using the biometric data.

Amended claim 23 recites:

An apparatus comprising:
a client comprising:
a crypto-API (application program interface) for receiving cryptographic function requests; and
a cryptographic service provider for establishing a secure connection to a remote crypto-server, and having the crypto-server generate a disposable public key/private key pair and perform the cryptographic function; and
a sensor for receiving biometric data from a user, the biometric data sent to the crypto-server to authenticate the user;
the remote crypto-server comprising:
a crypto-proxy interface for receiving a request for the cryptographic function from the client on the secure connection;
an authentication engine for authenticating the user based on the biometric data;
a cryptographic engine for performing the cryptographic functions; and
the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.

Applicants respectfully submit that Dulude does not teach generating a disposable public key/private key pair. Therefore, Applicants respectfully submit that claims 22 and 23, as amended, are not anticipated by Dulude.

The Office Action rejected claim 24 under 35 U.S.C. §102(e) as being anticipated by Dulude. Claim 24 recites:

An apparatus, comprising:
a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection;
an authentic engine to authenticate a user based on biometric data;
a cryptographic engine to use the user's private key, as a virtual smart card, to perform a requested cryptographic function; and
the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.

On page 7, lines 4-5, the Office Action states that "Dulude et al does not teach a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection." Thus, the Applicants respectfully submit that independent claim 24 and dependent claims 25 and 26 are patentable.

Applicants respectfully submit that in view of the amendments and discussion set forth herein, the applicable rejections have been overcome. Accordingly, the present and amended claims should be found to be in condition for allowance.

If a telephone interview would expedite the prosecution of this application, the Examiner is invited to contact Judith Szepesi at (408) 720-8300.

If there are any additional charges/credits, please charge/credit our deposit account no. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: OCT. 28, 2004

Sheryl Sue Holloway
Reg. No. 37,850

Customer No. 008791
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025
(408) 720-8300